REMARKS

Claims 1-23 are currently pending in the application. None of the claims have been amended.

Claims 1-23 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,324,683 ("Fuh"). Applicants respectfully submit that Fuh does not disclose, teach, or suggest every limitation recited in independent claims 1 and 13.

Independent claim 1 recites, in part, a system for debugging a computer application that employs rights-managed (RM) content, the system comprising a first, non-isolated process having the application and a shell version of a trusted component, such shell version of the trusted component receiving each request by the application for RM services and being unconcerned whether the debugger is monitoring the first process; and a second, isolated process separate from the first process and having a debugging version of the trusted component, the shell version of the trusted component in the first process forwarding the received request to the debugging version of the trusted component in the second process, such debugging version of the trusted component in the second process acting upon the request from the application in the first process, the debugging version of the trusted component in the second process also ensuring that the debugger is not monitoring the second process, the debugging version of the trusted component in the second process being unconcerned whether the debugger is monitoring the first process, whereby the debugger may monitor the application and the first process even as the application and first process are employing the RM content.

As stated in the present specification, a trust-based rights management system 30 allows an owner of digital content 32 to specify license rules that must be satisfied before such digital content 32 is allowed to be rendered on a user's computing device 34 (*Specification* at ¶ [0058]). For example, the content owner may wish to restrict the user from copying and re-distributing the digital content 32 to a second user, or may wish to allow distributed digital content 32 to be rendered only a limited number of times, only for a certain total time, only on a certain type of machine, only on a certain type of rendering platform, only by a certain type of user, *etc*. (*id*. at ¶ [0056]).

An application 42 that employs rights-managed digital content 32 typically includes or has local access to a rights management module, such as a trusted component 38, which may include a license evaluator 40 and an environment monitor 41 (*id.* at ¶¶ [0060], [0063] and [0065]). The application 42 and the trusted component 38 reside within a single process 44 (*id.* at ¶ [0065]). The trusted component 38 performs rights management functions in connection with the application 42, including license evaluation by way of the license evaluator 40 and environment monitoring by way of the environment monitor 41 (*id.* at ¶¶ [0060] and [0065]). Thus, the trusted component 38, by way of the environment monitor 41, ensures that the application 42 and the process 44 are not being monitored by an external element, such as a debugger 46, which may be employed by a nefarious entity to copy the naked content without any of the rights management protection associated with the digital content 32 (*id.* at ¶¶ [0020] and [0066]).

In certain situations, the debugger 46 should be allowed to monitor the application 42 and the process 44 if, for example, the application 42 and the process 44 are being developed and/or debugged by a legitimate developer (*id.* at ¶ [0067]). However, the legitimate developer will not be able to operatively couple the debugger 46 to the application 42 / process 44 for the reason that the environment monitor 41 and the trusted component 38 of the process 44, upon sensing the debugger 46, will prevent the legitimately debugging application 42 from having access to rights-managed digital content 32 (*id.*). Accordingly, in one embodiment of the claimed invention, the legitimate developer is provided with a shell version of a trusted component 38s that is run in a first process 44 and a debugging version of a trusted component 38d that is run in a second process 44 separate from the first process 44, thereby enabling the legitimate developer to use the debugger 46 with the application 42 that employs the rights-managed content 32 (*id.* at ¶¶ [0023] and [0068]).

In contrast, Fuh's objective, *inter alia*, is to provide a debugging method for external programs running under a client-server based relational database management system (RDBMS) (Fuh at col. 8, ll. 65-67). More specifically, a debugger is initiated from within a process running an external program by executing a special segment of code prior to the execution of the external program (*id.* at col. 9, ll. 15-18). This special segment of code includes a "debug" command which specifies a debugger to be invoked, identifies the process being debugged, specifies the directory of the source file of the external program being

debugged, informs the debugger to break at the specified function, and can redirect the debugger's input/output to a specified machine (*id.* at col. 9, ll. 18-24). Accordingly, Applicants respectfully submit that Fuh does not disclose a system for debugging an application employing rights-managed content at all, much less a system comprising a first, non-isolated process having a shell version of a trusted component that receives each request by the application for RM services and a second, isolated process having a debugging version of the trusted component that acts upon the request from the application.

Applicants further submit with respect to claim 1 that Fuh does not disclose that the shell version of the trusted component is unconcerned whether a debugger is monitoring the first process, nor does Fuh disclose that the debugging version of the trusted component ensures that the debugger is not monitoring the second process and is unconcerned whether the debugger is monitoring the first process, whereby the debugger may monitor the application and the first process even as the application and first process are employing the RM content.

In the Office Action, the Examiner contends that FIG. 14 of Fuh, and related text, disclose a system for debugging a computer application that employs rights-managed content (Office Action dated November 15, 2006 ("Office Action") at § 5, p. 3). Applicants respectfully disagree. FIG. 14 illustrates the environment of debugging a distributed Customer Information Control System (CICS) 6000 sample application (Fuh at col. 46, ll. 47-48). The CICS is a transaction monitoring system which provides a high level of efficiency for executing, including executing concurrently, thousands of multiple short running programs (*id.* at col. 2, ll. 24-27). As noted above, Fuh does not disclose or reference an application employing rights-managed content at all.

The Examiner further contends that FIG. 2, items 194, 181, 183, and related text, disclose a first, non-isolated process having the application and a shell version of the trusted component, and that FIG. 1, and related text, disclose a second, isolated process separate from the first process and having a debugging version of the trusted component (Office Action at § 5, p. 3). Applicants again respectfully disagree. FIG. 1 illustrates a RDBMS run-time environment in which the technology of user-defined functions, stored procedures and triggers are applicable (Fuh at col. 6, ll. 3-5). FIG. 2 shows an example of a client program 194 named "myclient" that executes a stored procedure 183 named "mysp" (*id.* at col. 6, ll.

52-53). Applicants respectfully submit that neither FIG. 1 nor FIG. 2 disclose a shell version or debugging version of a trusted component for performing RM services according to the limitations recited in independent claim 1.

Independent claim 13 is a method claim directed to substantially the same subject matter as independent claim 1. For example, claim 13 recites, in part, a method for debugging a computer application that employs rights-managed (RM) content, the method comprising a shell version of a trusted component being instantiated in a first, non-isolated process and a debugging version of the trusted component being instantiated in a second, isolated process, the application requesting the shell version of the trusted component to assist in decrypting and rendering the content, and the debugging version of the trusted component determining that the RM content is allowed to be rendered and decrypting the RM content. Therefore, claim 13 is believed to be allowable for at least the same reasons noted above with respect to claim 1.

For at least the foregoing reasons, Applicants respectfully submit that independent claims 1 and 13 patentably define over the cited reference and are, therefore, allowable. As claims 2-12 depend from claim 1, and claims 14-23 depend from claim 13, Applicants further submit that the dependent claims are also allowable for at least the reasons set forth above. Reconsideration of the Office Action and a Notice of Allowance are respectfully requested. In the event that the Examiner cannot allow the present application for any reason, the Examiner is encouraged to contact the undersigned attorney, Joseph R. Condo at (215) 564-8977, to discuss resolution of any remaining issues.

Respectfully submitted,

Date: February 15, 2007

/Joseph R. Condo/
Joseph R. Condo
Registration No. 42,431

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439